

Report 2017

of the .ch Registry

SWITCH



Management Summary/Highlights	
Security and stability as a priority	3
Activity report – operations	
.ch: 30 years of security and stability	4
Fighting cybercrime	6
Community	7
Data Escrow	8
Activity report – innovations	
DNSSEC	9
DNSSEC Key ceremony	10
SWITCH DNS firewall	11
Replacement database server	12
Emergency drill	13
Fraudulent webshops	14
ISMS recertification	15
Changes for registrars	16
ICT Law Working Group	17
Activity report – statistical indicators	
Domain name inventory – Developments 2017	18
Market share of .ch and .li	19
DNSSEC developments	20
Dispute resolution	22
Registrar developments	23
Name server performance	24
Battling cybercrime: quantitative	25
Battling cybercrime: qualitative	26
Quality of the malware process	27
Activity report – economic indicators	
Economic indicators 2017	28
Activity report – planned development of the .ch domain	
Strategic orientation 2018	29
Planned innovations 2018	31
Growth forecast 2018	32



*Urs Eppenberger
Head of Registry, SWITCH
(Photo SWITCH)*

SECURITY

and stability as a priority

Uninterrupted, secure operations for all services

From the point of view of registrars and domain name owners, the stable, secure operation of the registry is absolutely key. And that's why this is our top priority at SWITCH. Maintenance and expanded functionality require interventions and changes in the whole system, but these are carefully tested and planned.

This means we were able to put the following technical developments in place:

- Implementation of the data escrow
- Replacement of database infrastructure

Information security

Data, infrastructure and processes are particularly valuable to a registry. And that's why we take particular care to protect them. Recertification under ISO 27001 shows that security isn't just a watchword for SWITCH but, rather, a continuous process of improvement that we live day in, day out.

Critical infrastructure such as the registration system and the DNS are implicit targets for attack. There is an increased risk of politically motivated acts, something that a number of registries throughout Europe have encountered in the last two years. SWITCH has carried out technical measures at the network level to prevent DDoS attacks. But just as important is training for our employees. We staged an emergency drill which used a genuine DDoS attack to test the interaction of network, security and application experts. A DDoS attack

cannot be prevented, but technical tools and trained personnel can reduce the risk of damage to the registry.

Fraudulent webshops

Based on the scope for action that OFCOM provides to act against suppliers of counterfeit branded products on .ch websites, SWITCH cooperated with law enforcement authorities in a concerted campaign to revoke the domain names of 6,093 fraudulent webshops.

Status of ccTLD .ch

Domain names in the national ccTLD .ch remain attractive, even with a wide range of alternative domain endings. For users, .ch offers a secure place with a connection to Switzerland. We are continuously and actively combating malware and phishing based on the information that is aggregated and analysed via the network of the SWITCH-CERT security team. The registrars and hosts have drawn up processes that ensure rapid action for the benefit of their customers. And that's how to maintain a worldwide top ranking. This success comes from successful cooperation between the federal government, authorities, SWITCH and IT service providers.

Awareness

SWITCH has created a new position for security awareness. Proactive measures that will be drawn up in this area will allow us to further contain misuse.

.ch

30 years of security and stability

On 20 May 1987, ETH professor Dr Bernhard Plattner entered 'ch' in the domain name system, marking the start of the internet in Switzerland.

Over the next 30 years, SWITCH not only established the internet in Switzerland but also made .ch Europe's most secure address.

The press release:

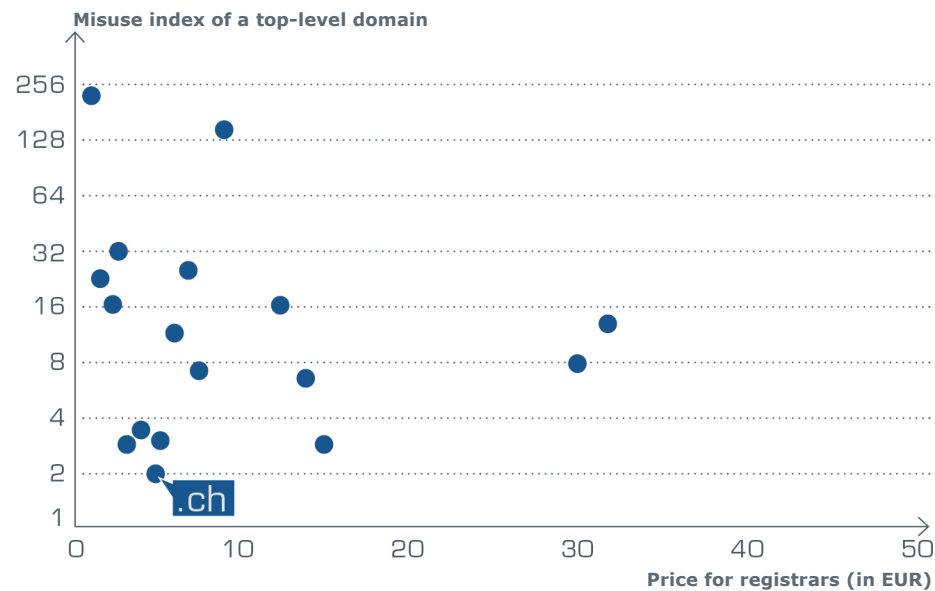
<https://www.switch.ch/news/30years-ch/>



Prof. Dr. Bernhard Plattner
ETH Zurich
(Photo ETH Zurich/Inken De Wit)

.ch

30 years of security and stability



PRICE/SECURITY RATIO

Of the European registries with open policies, .ch took first place when it came to security.

Figures: Architelos

When cybercriminals search for top-level domains for their own underhand purposes, they are particularly drawn to those with low prices and open registration policies. By that reckoning, .ch would be highly attractive for internet crime, since both of these criteria apply to this top-level domain.

US internet analysis specialists Architelos investigated misuse on websites (malware and phishing) throughout Europe and arranged them by top-level domain. When it came to security, .ch took first place.

→ Statistical indicators on the battle against cybercrime can be found on page 25.

FIGHTING CYBERCRIME

In 2017, we continued our measures to combat cybercrime.

Phishing

Phishing remained a problem in 2017. Cybercriminals use both compromised websites as well as domain names used solely for phishing. Our partnership with MELANI as a recognised organisation gained traction.

Drive-by/Malware

The use of drive-by and malware has declined since the previous year.

→ Statistical indicators on the battle against cybercrime can be found on page 25.

Swiss correspondence addresses

The number of requests for Swiss correspondence addresses from Swiss authorities under Art. 16 increased greatly. Here, SWITCH works closely with various bodies to speed up detection of improper registrations with false or stolen identities, and to check the identity of owners.

Cryptocurrencies

Recently, .ch websites have also been misused for mining cryptocurrencies.

The blog post:

<https://securityblog.switch.ch/2017/10/05/money-for-nothing-and-coins-for-free/>

COMMUNITY

Anycast service

In January 2017, a third DNS Anycast service – CommunityDNS – was launched for the .ch-zone. This means there are an additional 200 nodes in 50 locations all contributing to the resistance against DDoS attacks. SWITCH hosts one of these nodes at the Swiss Internet Exchange, providing network operators in Switzerland with a direct link for rapid response times.

Cybercrime Awareness

On 10 April 2017, the Zug police staged an awareness evening for the public. At the event, the SWITCH-CERT expert team supported the police as a contact point for questions from the public.

Swiss Web Security Day

On 19 October 2017, SWITCH joined up with simsa and SISA to launch Swiss Web Security Day in Lucerne. The goal of the meeting was to raise awareness of security issues.

There were 59 participants – registrars, web hosts, and representatives from associations, telcos, banks and public bodies.

dialog@switch

On 16 November 2017, SWITCH hosted a meeting with registrars. We shared information on planned developments and coordinated these with their requirements.

There were 18 attendees from 11 registrars. Our thanks to OFCOM, particularly Olivier Girard and Michael Strasser, for their talk on the new OID.

DATA ESCROW

On 1 February 2017, SWITCH concluded a data backup agreement with the Rümlang-based company Netcloud. Each day, the organisation backs up data from the registries in line with OFCOM provisions, structured according to current ICANN practice.

In 2017, the daily data escrow of the .ch domain registration and administrative systems ran smoothly.



*DATA CENTRE
Netcloud, Rümlang
(Photo e-Shelter)*

DNSSEC

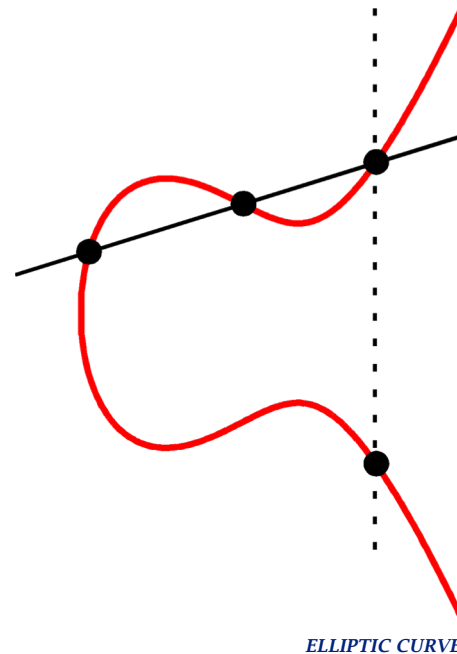
Crypto-algorithms

SWITCH has prepared for signing with modern elliptic curves (ECDSA) in the .ch zone. However, the IANA root zone management system wasn't ready for this type of signature by the 2017 key ceremony, and SWITCH had to postpone the conversion until 2018.

The option of lodging Edwards-curve DS records (EdDSA) for .ch domain names has been available since March 2017.

Promotion of DNSSEC signing and validation

In a number of talks at relevant conferences, SWITCH outlined the importance of DNSSEC. Organisations such as hosting providers, universities and banks were each encouraged to sign their domain names and given expert support.



Simplification of signing

We also launched the project 'Automated DS update'. This will enable owners to secure .ch domain names with DNSSEC with no manual interaction required.

Analysis tools

With the acquisition of big data applications, it is now possible to analyse queries to .ch name servers over extended periods and to thereby approach operators of non-validating resolvers directly, for instance.

DNSSEC

Key ceremony

For 2017, we adapted the ceremony to current requirements.

- Allotment of .ch and .li in independent procedures and data containers
- Separation of ceremony operating system and data containers
- Key-holders increased from three to five
- Distribution algorithm changed (Shamir's Secret Sharing Algorithm)
- Preparation for conversion to ECDSA (see previous page)
- As required, an OFCOM representative took part in the key ceremony as official key-holder.

The story:

<https://swit.ch/key-ceremony17>



*DNSSEC
Key ceremony at SWITCH*

SWITCH DNS FIREWALL

SWITCH uses its own DNS firewall to protect its internal infrastructure. A service that began as a university project now enjoys great popularity with other customer groups.

At present, there are more than 220,000 users from a total of 30 organisations.

DNS firewall features

Prevention: By blocking access to infected/malicious sites, the SWITCH DNS firewall can counteract infections and data outflow and the damage they cause.

Detection: SWITCH can detect computers that are already infected.

Awareness: A parameterised landing page creates greater awareness in end users when accessing malicious internet pages.

REPLACEMENT

database server

New Oracle database in operation

In September 2017, SWITCH put new hardware and software into operation for the .ch and .li registries. The current Oracle database was installed and outdated hardware taken out of operation.

We tested extensively prior to this conversion, with a number of SWITCH teams as well as external partners taking part.

The upgrade was carried out during a scheduled maintenance window, so that the registrars did not experience any unplanned interruptions.



DATABASE SERVER
Sample image
(Photo SWITCH)

EMERGENCY DRILL

Emergency DDoS attack drill on EPP server

A number of registries have been subject to DDoS attacks over the last two years. In each case, a political motive was suspected. MELANI issued a warning to this effect.

In line with this realistic scenario, SWITCH carried out an emergency drill on its test system. A DDoS attack always begins with the failure of the targeted system. Indeed, the EPP test system also failed during a realistic attack.

Multiple SWITCH teams worked on countermeasures and information to the registrars and other stakeholders, using the exercise scenario that it was the operating system rather than just the test system that had failed.

The results of the emergency drill were analysed and produced the following positive outcome: the SWITCH incident management concept can be used in these situations as well, and the employees used its processes carefully in the staged emergency situation.



INCIDENT SEQUENCE

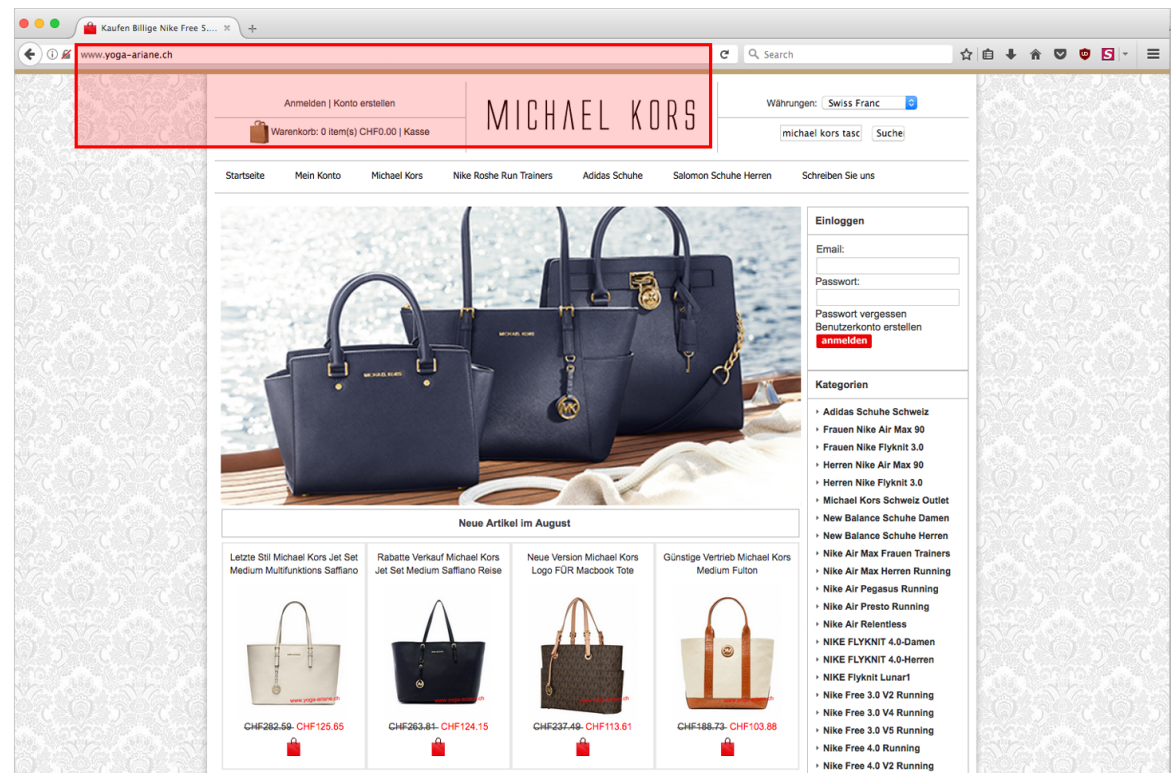
FRAUDULENT WEBSHOPS

In February 2017, SWITCH introduced an automated process for determining Swiss correspondence addresses where fraudulent websites were suspected.

Since the beginning of this process, queries from Swiss authorities in 6,130 cases resulted in demand for Swiss correspondence addresses. In 37 cases, the owner got in touch and supplied a valid Swiss address. In the other 6,093 cases, the domain name was revoked in line with the Ordinance on Internet Domains, Art. 16.

The story:

<https://swit.ch/fakewebshops>



EXAMPLE OF A FRAUDULENT WEBSHOP

One warning sign is a mismatch between the internet address and the name of the webshop

ISMS RECERTIFICATION

In 2017, SWITCH successfully recertified the registry for domain names under ISO 27001. The certificate is valid until December 2020.

This confirms that SWITCH and the registry are achieving the desired success in their ongoing efforts to maintain and improve the security and stability of .ch and .li.

The story:

<https://swit.ch/pyqsr>



ISO 27001
certificate for the SWITCH registry

CHANGES

for registrars

Changes to subscription periods

Initial registrations are now calculated to the day.

Let's assume a subscription period from 14/07/2017 to 13/07/2018. Previously, the registrar would not be charged for the first partial month, as the subscription would not begin until the following month if registering on 14/07/2017 (subscription period: 01/08/2017 to 31/07/2018).

Flexible solution for lapsed subscriptions

A registrar can delete a domain name up to 10 days after the subscription has lapsed. The amounts already charged are credited to the registrar in the following month.

For new registrations, this practice of 10 days' grace period has already existed for some time. This means the registrar can process payments from customers that arrive after the subscription has lapsed – and retain the customer.

Registrars value this function highly.

ICT LAW WORKING GROUP

Purpose of the ICT Law Working Group

SWITCH established the ICT Law WG 10 years ago. Legal consultants from Swiss universities use the working group's meetings to raise ICT-related questions. There were two meetings in 2017, with a representative from the SWITCH legal department present on each occasion.

New Telecommunications Act and Surveillance Act

At the first meeting in Olten on 12 June 2017, hosts FHNW, solicitor Simon Schlauri and the UZH discussed the Telecommunications Act (TCA) and the Federal Act on Post and Telecommunications Surveillance (BÜPF).

General Data Protection Regulation (GDPR)

At the second meeting on 13 September 2017, it was SWITCH's turn to host. The topic was the General Data Protection Regulation (GDPR) and what it means for Swiss universities. Maria Winkler and Dr Robert Weniger gave talks on the implementation of the GDPR as well as developments in European data protection and the cantonal legislation.

DOMAIN NAME INVENTORY

Developments 2017

Development of .ch

The inventory of .ch domain names increased by a good 90,000 within a year.

Development of .li

The inventory of .li domain names decreased by almost 1,000 within a year.

	2016		2017	
	.ch	.li	.ch	.li
New registrations	280,721	9,207	283,576	8,619
Deletions	255,708	9,484	215,730	10,147
Reactivations*	27,548	502	21,017	391
Domain inventory as at 31/12	2,034,509	63,466	2,123,372	62,587

DOMAIN NAME INVENTORY

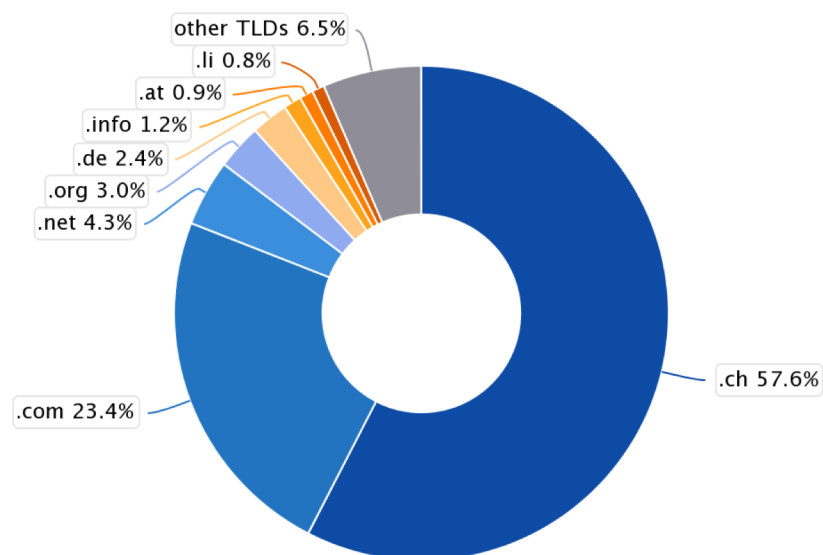
Development of the domain name inventory for .ch and .li

** Deleted domain names which were reactivated by registrars within the 40-day transition period*

MARKET SHARE

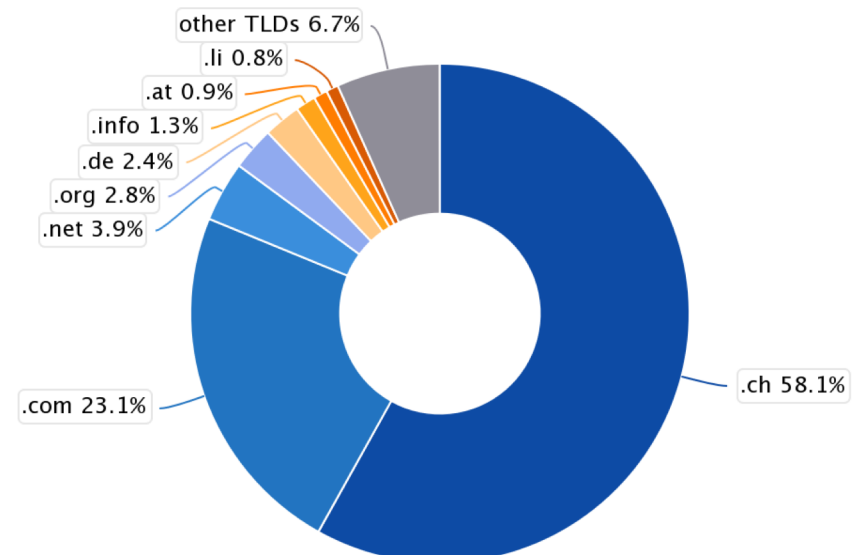
of .ch and .li among Swiss domain name owners

The market share of .ch domain names among owners in Switzerland increased by 0.5% between January 2017 and January 2018.



MARKET SHARES JANUARY 2017
of various TLDs among domain
name owners in Switzerland
Source: CENTR

There was a slight loss in market share for the older, generic TLDs .com, .net and org. There was no significant change to .li domain names in the same period.



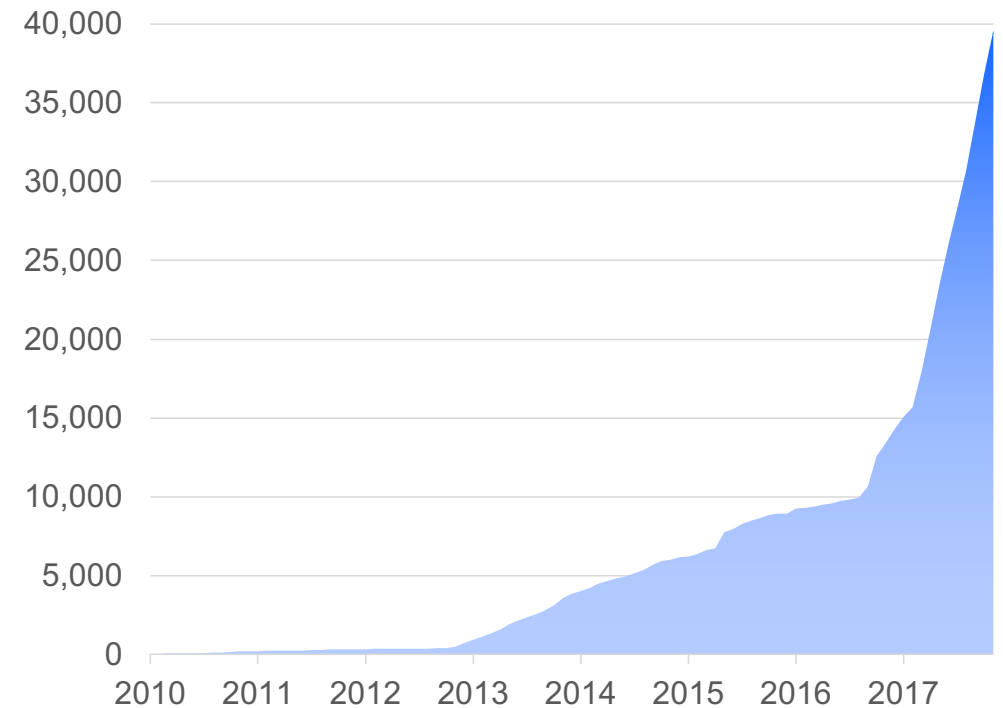
MARKET SHARES JANUARY 2018
of various TLDs among domain
name owners in Switzerland
Source: CENTR

DNSSEC DEVELOPMENTS

Number of signed domain names

In 2017, the number of .ch domain names signed with DNSSEC (39,581) tripled in comparison to 2016 (13,412).

This remarkable increase is largely attributable to the fact that individual registrars have begun automatically signing all new domain names with DNSSEC.

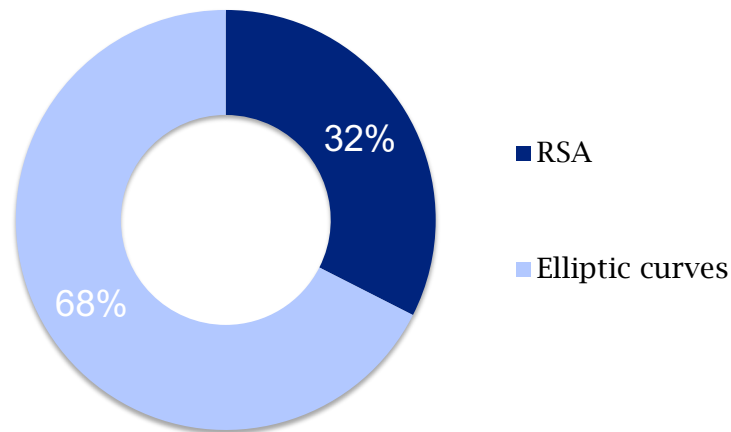


DNSSEC
Number of .ch domain names
signed with DNSSEC

DNSSEC DEVELOPMENTS

Distribution of DS algorithms

Almost 70% of the .ch domain names protected with DNSSEC use modern ECDSA (elliptic curve) signatures, while 30% use traditional RSA signatures.



SHARE OF DNSSEC ALGORITHMS

DNSSEC algorithm	Number	Share
5 - RSASHA1	186	0.47%
7 - RSASHA1-NSEC3-SHA1	11,035	27.72%
8 - RSASHA256	1,669	4.19 %
10 - RSASHA512	37	0.09 %
13 - ECDSAP256SHA256	26,866	67.50 %
14 - ECDSAP384SHA384	8	0.02%
15 - ED25519	1	0.00%

DNSSEC SIGNATURES USED

DISPUTE RESOLUTION

Since 2004, SWITCH has been using the dispute resolution service of WIPO (World Intellectual Property Organization).

In 2017, there were just 14 cases to process. The long-standing rule of thumb is around 30 cases. This is what we anticipate for the future as well.

WIPO operates a dispute resolution service accredited by ICANN for over 70 other registries.

	2016	2017
Domain name transferred to applicant	22	11
Complaint rejected	2	3
Number of proceedings	24	14

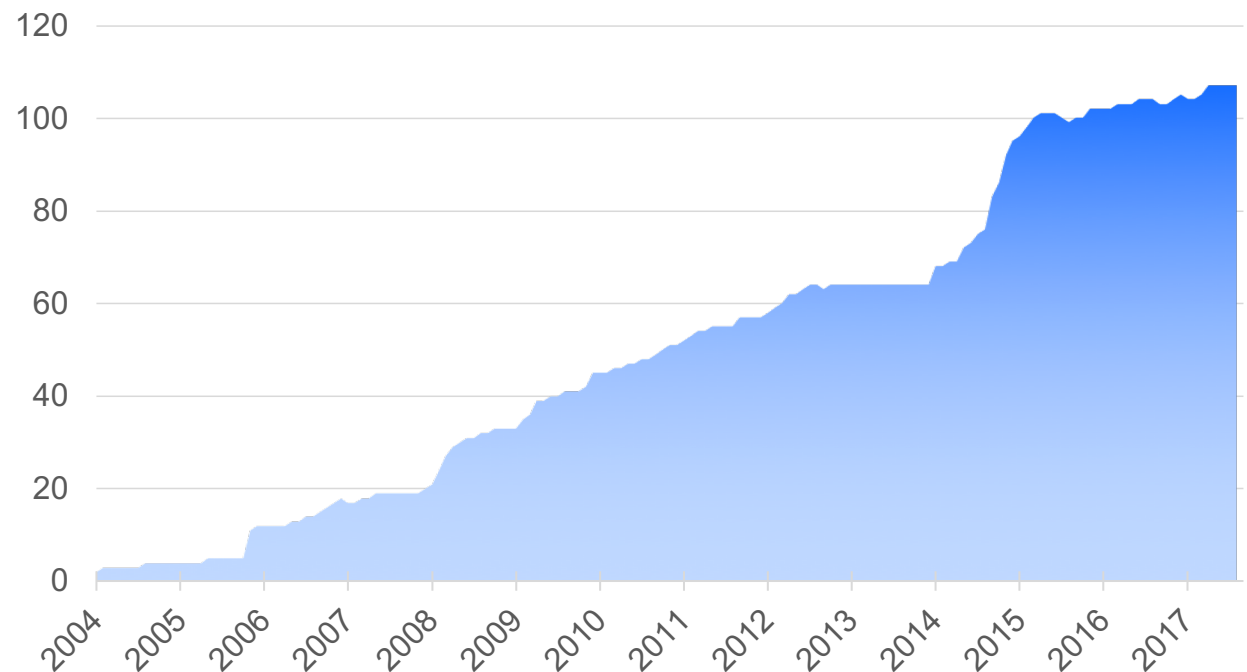
DISPUTE RESOLUTION
Comparison of number of cases decided

REGISTRAR DEVELOPMENTS

With the announcement of domain name migration from SWITCH to the registrars, the number of registrars leapt from 83 to 100 in 2015. More hosting and email providers wanted to become registrars so that they could manage their customers' domains themselves in the future.

This trend slowed a little, and SWITCH had 104 active registrars by the end of 2016.

There were only three additional registrars in 2017. We believe the supplier market is saturated, and we anticipate no major changes in 2018.

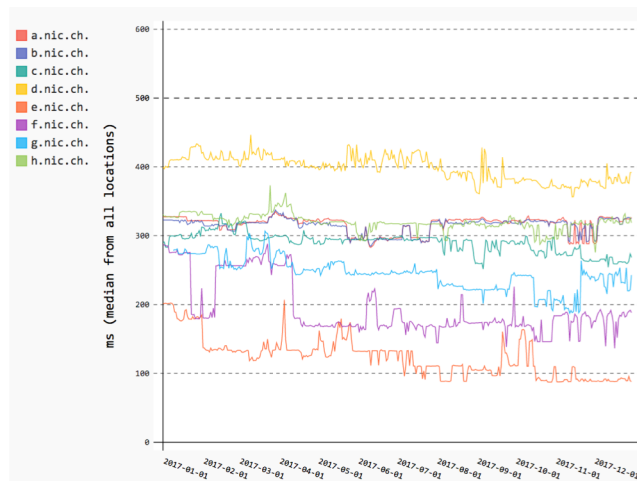


INVENTORY DEVELOPMENT
By the end of 2017, the registry counted 107 active registrars

PERFORMANCE

of the name servers

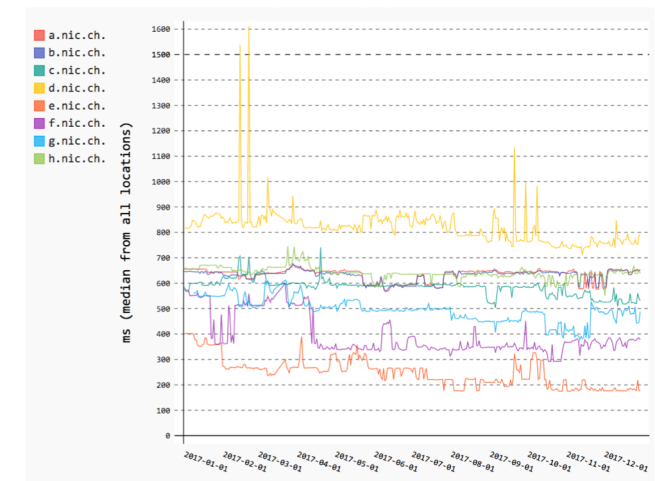
In terms of DNS performance measurement, SWITCH relies on the response time requirements for DNS queries stipulated by the ICANN Agreement; queries in the CH zone must be answered by at least one logical name server within 500 ms (UDP) or 1500 ms (TCP).



UDP RESPONSE TIMES
Combined response times of IPv4 and IPv6

In 2017, this requirement was met in each instance. The measurements were carried out by RIPE and are available to the public at <https://atlas.ripe.net/dnsmon/group/ch>.

Unicast a.nic.ch (CH), b.nic.ch (CH), c.nic.ch (USA), d.nic.ch (BR), h.nic.ch (CH)
Anycast e.nic.ch, f.nic.ch, g.nic.ch



TCP RESPONSE TIMES
Combined response times of IPv4 and IPv6

FIGHTING CYBERCRIME

quantitative

In the reporting year, we captured and processed the following cases:

	# malware cases	# phishing cases
Reports received	1,636	952
Suspicion confirmed	659	325
Number of blocked domain names	219	75
Reason for lifting block:		
- statutory period expired:	33	4
- lifted after block:	155	33
- in process at reporting day:	3	7
Revoked domain names	28	36

NUMBER OF MALWARE AND PHISHING CASES 2017
Quantitative view

FIGHTING CYBERCRIME

qualitative

The time spent on cases was:

	Duration	
Duration of the block Pursuant to OID Art. 15, 1,2,3 max. blocking time 30 days (720 hours)	Min. time	1.07 h
	Average	95.53 h
	Max. time	162.20 h
Response time from SWITCH following notification	Average	15.09 h
Time until removal of threat following notification to the owners	Average	78.45 h

NUMBER OF MALWARE AND PHISHING CASES 2017

Qualitative view

QUALITY

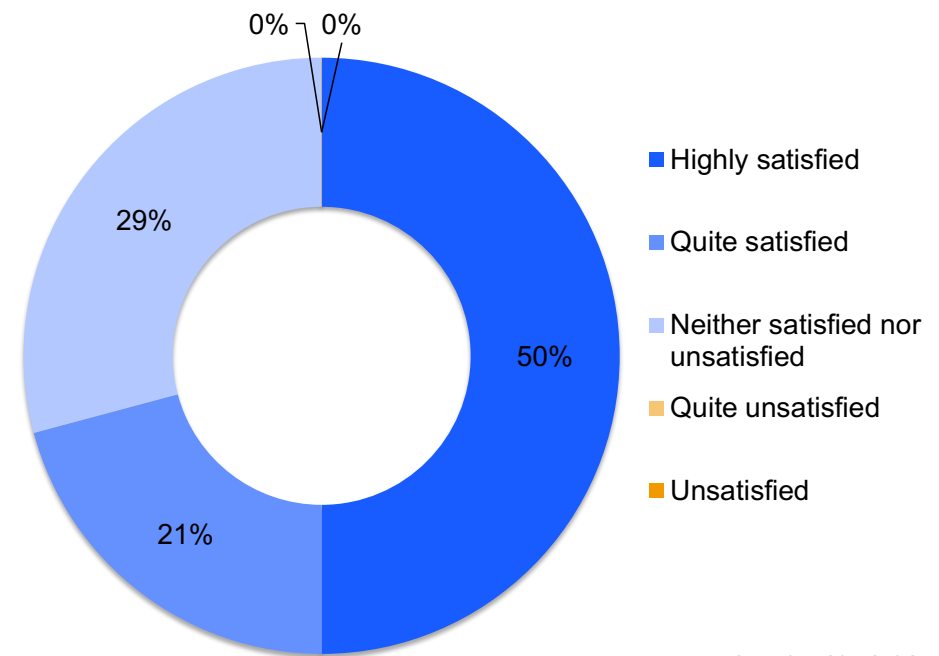
of the malware process

At the heart of the security efforts surrounding the .ch top-level domain lies the malware process. This is an efficient, well-oiled, joint procedure against internet crime that brings together SWITCH, the authorities and registrars. This process has been enshrined in the law since 2010.

When malware is reported on .ch websites, SWITCH notifies the domain name owners of the infected sites.

To enable ongoing improvements in measures against internet crime, SWITCH carries out continuous quality checks for the malware process among participating parties. Once the malware process is finished, SWITCH asks all domain name owners

to evaluate the quality of the malware process. In 2017, 984 affected domain name owners underwent the malware process. Of these, 29 filled out the survey.



OVERALL SATISFACTION
Over 70% of all respondents were satisfied or highly satisfied with the malware process

ECONOMIC INDICATORS

The Foundation Council session on 7 June 2018 will pass the SWITCH foundation's 2017 Report, along with the balance sheet and income statement. Dispatch and publication will be on 8 June 2018.

No figures will be published at this point. Instead, interested parties will be referred to the comprehensive documents of the 2017 SWITCH Annual Report.

STRATEGIC ORIENTATION 2018

1/2

Lasting appeal

The top-level domains .ch and .li have open policies. For registrars, there are minimal barriers to becoming part of the supplier chain. Resellers have the option of offering services with even less technical effort of their own via specialised registrars. With the competitive wholesale price and the low barriers for providers and interested parties, the top-level domain .ch has major appeal in the Swiss market.

An analysis of the top-level domain names used by Swiss owners shows the extremely strong position of .ch. Companies that are active internationally secure an additional .com domain name. The new TLD .swiss assumes an important, quantitative yet subordinate role. In the European environment, the growth of country-

specific TLDs is declining. This trend is not so apparent in Switzerland; with the transfer of direct customer business from SWITCH to the registrars, caution must be exercised when using 2016 figures for forecasts.

With these factors in mind, we can assume a growth rate of around 4% for 2018.

Battling cybercrime

Low prices and an open registration policy make .ch attractive for cybercriminals. The OID provides the registries with the right tools for making the TLD a secure place for their users. However, the costs associated with securing .ch are constantly increasing.

STRATEGIC ORIENTATION 2018

2/2

European Data Protection Law

The registry operates in the Swiss legal sphere. However, the new European Data Protection Law affects a range of registrars directly. The consequences are still a subject for discussion in European registries. If they can reach a common set of principles, then it is worth at least seeing if those principles should be adopted. That would certainly make the registrars' lives easier. Presently, however, there is no sign of a unified solution. This is something that remains to be seen in the course of 2018.

Checking content

Various interest groups are currently increasing pressure on internet providers to check content and, where necessary, remove it from the internet.

The focus is also on social networks and the use of hate speech. The discussion is conducted openly and registries in particular are seen as instruments of change.

Switzerland has the advantage of the OID, a balanced regulation that doesn't overshoot the goal but still offers an important statutory framework for the fight against cybercrime. The goal will be to make this pragmatic approach better known with clear responsibilities, particularly in the European environment. There must be countermeasures to the obligation to check content or delete domain names on a mere tip-off from third parties, so that the legal risks for registries and registrars, as well as the associated expenses, remain manageable.

PLANNED INNOVATIONS 2018

Securing important domain names

Since the customer migration, all domain names are managed by registrars. That includes domain names with high public visibility, with high revenues on online platforms, or with connections to important infrastructure in Switzerland.

With the ‘registry lock’ function, a registrar can secure a domain name with a registry in such a way that it can only be managed in an offline process. This secures domain names against manipulation and targeted attacks.

Cryptographic keys in the DNS

The cryptographic keys for DNSSEC are managed by the same organisation that operates the name server for the domain in question. That could be the registrar, the

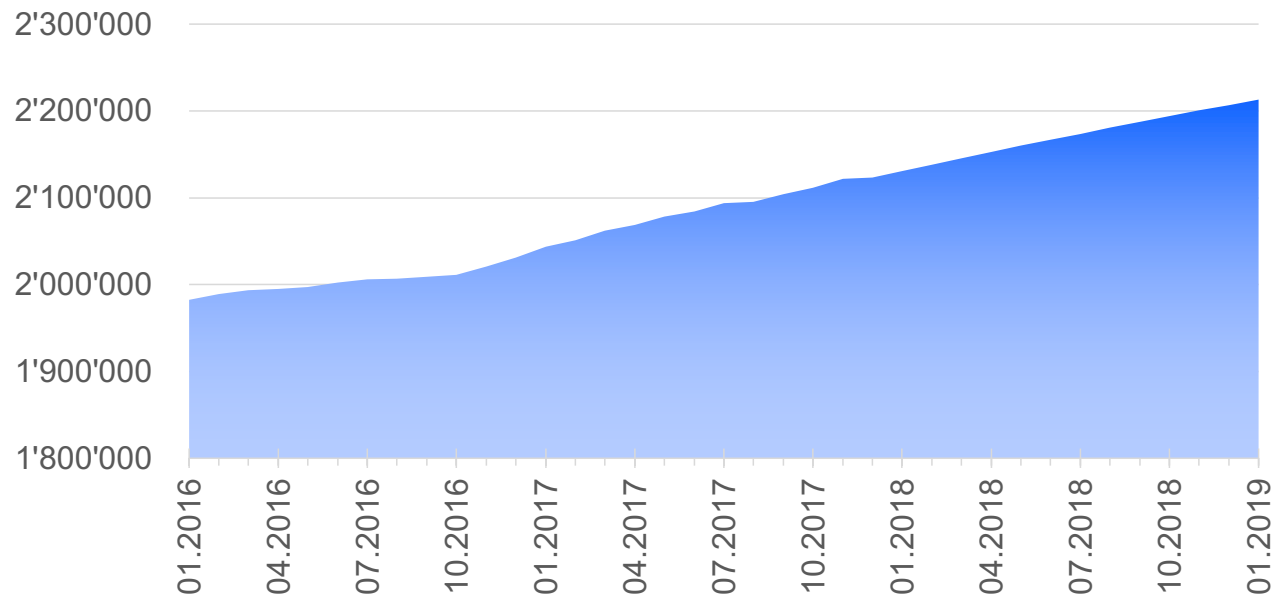
host, or even a private individual. To date, the key always had to be registered through a registrar or registry. Only a few registrars support DNSSEC. But the interest is increasing.

Through the ‘CDS/CDNSKEY’ mechanism standardised in the RFCs 7344 and 8078, keys can be registered directly with the registry via DNS. The technology has proven itself, although in Europe it is so far only used in the TLD .cz. With this second route, interested parties have the option of automatically protecting their self-managing domain names in particular with DNSSEC.

GROWTH FORECAST 2018

.ch domain names

SWITCH is forecasting growth of 4% for 2018. This represents an average increase of around 7,500 domain names per month.



GROWTH FORECAST
.ch domain name inventory 2018



SWITCH
Werdstrasse 2
Postfach
CH-8021 Zürich

Telefon +41 44 268 15 15
www.switch.ch
info@switch.ch

SWITCH

Working for a better digital world

